моженных органов. Об этом свидетельствует ежегодный рост количества выявленных и пресеченных попыток передачи им незаконного денежного вознаграждения (взяток). В то же время организация процесса противодействия коррупции в системе таможенных органов — процедура весьма сложная. Реализация инициатив, закрепленных в нормативных правовых актах, требует не только привлечения государственных ресурсов, но и активизации всего общества для решения этой проблемы.

Список основных источников

1. Василевич, Г. А. Противодействие коррупции — одна из главных задач государства и общества / Г. А. Василевич // Научно-практический журнал «Право.by». — 2014. — № 5. — С. 5–11.

2. Договор о Таможенном кодексе таможенного союза [Электронный ресурс] [подписан в г. Минске 27.11.2009 г.] // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. — Минск, 2017.

3. О борьбе с коррупцией [Электронный ресурс] : Закон Респ. Беларусь, 20 июля 2006 г., № 165-З // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. — Минск, 2017.

4. О борьбе с коррупцией [Электронный ресурс] : Закон Респ. Беларусь, 15 июля 2015 г., № 305-З // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. — Минск, 2017.

УДК 343.985.3:004(477)

К. Ю. Исмайлов

заведующий кафедрой кибербезопасности
и информационного обеспечения
Одесского государственного университета
внутренних дел, кандидат юридических наук (Украина)

НЕКОТОРЫЕ ОСОБЕННОСТИ ИЗЪЯТИЯ КОМПЬЮТЕРНОЙ ТЕХНИКИ ВО ВРЕМЯ ПРОВЕДЕНИЯ ОБЫСКА (ОСМОТРА)

Развитие и распространение современных информационных технологий способствовали созданию предпосылок для роста преступности, связанной с неправомерным доступом к компьютерным

сетям, несанкционированным получением или изменением информации, незаконным использованием и распространением компьютерного программного обеспечения. В силу своей специфичности данный вид преступления имеет высокий уровень латентности и низкий уровень раскрываемости.

В связи с быстрым темпом компьютеризации общества у работников Национальной полиции Украины возникают трудности с отсутствием полной обоснованной методики расследования компьютерных преступлений и проведения отдельных следственных действий, в частности изъятия компьютерной техники и электронных доказательств, которые содержатся на ней [1].

Итак, когда необходимые органам расследования доказательства содержатся на компьютерах, то, чтобы провести обыск, обеспечив законность и доказательную базу, всегда необходимо привлекать специалиста, у которого есть специальные знания, а самое главное — специализированная, лицензированная техника для этого. Следователь, хотя и обладает достаточными навыками и знаниями в области компьютерной техники и информационных технологий, без помощи специалиста может допустить ошибки при осмотре технической аппаратуры, снятии необходимой информации и (или) ее изъятии, что приведет к необратимым последствиям [2].

Значимая для расследования информация может находиться на магнитных дисках, компакт-дисках (CD), DVD-дисках, флешнакопителях, оптических дисках, магнитных карточках, цифровых кассетах и т. д. Такие носители могут содержаться в персональных компьютерах, серверах, коммуникационном оборудовании, коммуникаторах, смартфонах, мобильных телефонах, цифровых фотоаппаратах и видеокамерах, плеерах и другой подобной технике — вся такая техника со встроенными носителями изымается целиком. Так, серверные необходимо сразу же взять под контроль, так как возможно дистанционное управление ими, что приведет к потере данных.

Следует помнить, что техника стремительно развивается и доступные пользователю носители могут завтра появиться в составе таких устройств, которых еще нет сегодня. В ближайших планах производителей — оснастить встроенными компьютерами всю бытовую технику: холодильники, кондиционеры, кофеварки, стиральные машины и прочее. Компьютер в составе бытовой техники

скорее всего будет включать встроенный или с возможностью трансформации носитель и сетевой интерфейс для удаленного доступа.

Кроме того, для обеспечения возмещения причиненного вреда может понадобиться обнаружение и изъятие кошельков с криптовалютами (Bitcoin, Ethereum и другие).

При извлечении компьютерной техники не должна меняться никакая информация, содержащаяся на носителях, которые являются изъятыми. Следователь должен доказать, что представленная эксперту или суду компьютерная информация не менялась ни в процессе обыска, ни при последующем хранении [3].

Доступ к информации и исследование ее на месте допустимы лишь в тех случаях, когда невозможно изъять носитель и отправить его на экспертизу. Такой доступ должен проводиться компетентным специалистом, который может понять и дать объяснение каждому своему действию.

В момент изъятия компьютерной техники следователь должен взять под контроль помещения, где установлена техника, а также электрощит, не позволять никому, кроме компетентного специалиста, прикасаться к технике и устройствам электропитания. Всю подключенную к компьютеру периферию следует сфотографировать или описать в протоколе, чтобы было понятно, какие были соединения.

Также стоит обратить внимание на место, где находится компьютерная техника, т. к. рядом могут быть записаны пароли, сетевые адреса и другие данные (часто такие записи лежат рядом, приклеены к монитору, висят на стене).

Если принтер что-то печатает, необходимо дождаться окончания печати. Все, что находится в исходном лотке принтера, описывается и изымается наряду с другими носителями компьютерной информации. После этого компьютеры надо выключить, это должен сделать специалист.

Изъятая техника упаковывается в зависимости от хрупкости и чувствительности к внешним воздействиям. Особенно чувствительны к вибрации жесткие магнитные диски; их механическое повреждение (например, через перевозки в багажнике) приводит к полной недоступности данных. Необходимо внимательно осмот-

реть дверные проемы на предмет наличия устройств для размагничивания.

Кроме этого необходимо опросить всех пользователей на предмет знания паролей. Стоит узнать у каждого сотрудника все известные ему пароли, имеющие отношение к удаленной технике. Пароли не следует воспринимать на слух, их надо записать по символам, обращая внимание на алфавит и регистр каждого символа, и выверить. После выполнения всех необходимых вышеуказанных действий в конце протокола указываются заявления присутствующих при осмотре и ставятся соответствующие подписи [4].

Еще одной важной проблемой при обысках, осмотрах является практическая неосведомленность прокуроров, осуществляющих процессуальное сопровождение и поддержку государственного обвинения в суде, по преступлениям, которые совершаются в киберпространстве. Чтобы исправить эту ситуацию, необходимо ввести в учебные планы подготовки прокурорских кадров дополнительные дисциплины, а с действующие прокурорами проводить тренинги.

Итак, практическое значение вышеупомянутого материала является достаточно весомым, т. к. состоит в выделении конкретных рекомендаций и тактических действий при проведении осмотра изъятой компьютерной техники при расследовании компьютерных преступлений, которые позволят качественно получать доказательную базу и эффективно расследовать уголовные производства.

Список основных источников

1. Бутузов, В. М Злочини із застосуванням сучасних інформаційних технологій // Боротьба з організованою злочинністю і корупцією (теорія і практика). — 2003. — № 7. — С. 84–89.

2. Касаткин, А. В. Тактика сбора и использование компьютерной информации при расследовании преступлений: дис. … канд. юрид. наук : 12.00.09 / А. В. Касаткин. — М., 1997. — 215 л.

3. Зачек, О. І. Особливості розкриття та розслідування кіберзлочинів : метод. рекомендації / О. І. Зачек, В. В. Навроцька, І. А. Федчак. — Львів : Львівський державний університет внутрішніх справ, 2010. — 60 с.

4. Федотов, Н. Н. Форензика — компьютерная криминалистика / Н. Н. Федотов. — М. : Юридический Мир, 2007. — 217 с.